



«Под капотом» PT X

Технологии, которые не дают атакам пройти незамеченными

Профиль угроз



33%

успешных кибератак
в России совершаются
финансово
мотивированными
группировками

Профиль угроз



33%

успешных кибератак
в России совершаются
финансово
мотивированными
группировками

4 часа

Достаточно для реализации
ущерба после получения
контроля над доменом

Профиль угроз



33%

успешных кибератак
в России совершаются
финансово
мотивированными
группировками

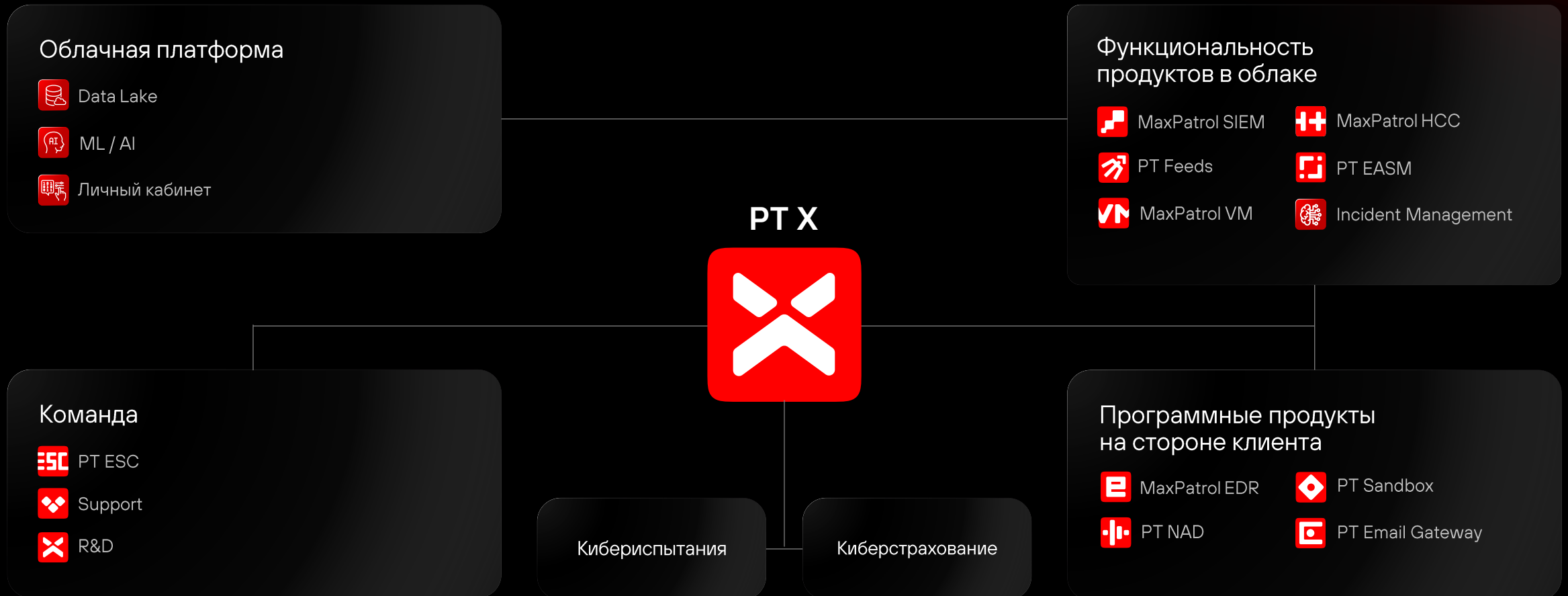
4 часа

Достаточно для реализации
ущерба после получения
контроля над доменом

147 млн
руб.

Требуемый выкуп
в среднем запрашивают
киберпреступники
у своих жертв

Архитектура PT X



РТ X сегодня



32

клиента

22

выбрали версию PRO

5

АРТ-группировок
выявлено и остановлено

3

zero-day-атаки
остановлено

в них использовались ранее
неизвестные уязвимости

Кейс № 1.

Атака через мисконфигурации



Атака

Цепочка атаки через внешнюю уязвимость



SSO endpoint
/app/superset/
tekon/php



Apache Superset

- JWT с правами all_database_access
- SQL Injection для доступа к служебным БД

Защита

Кейс № 1.

Атака через мисконфигурации



Атака

Цепочка атаки через внешнюю уязвимость



SSO endpoint
/app/superset/
tekon/php



Apache Superset

- JWT с правами all_database_access
- SQL Injection для доступа к служебным БД

Защита

- РТ EASM обнаруживает внешнюю уязвимость за 71 день до атаки (CWE-1220, CWE-89, CWE-266)

Кейс № 1.

Атака через мисконфигурации



Атака

Цепочка атаки через внешнюю уязвимость



SSO endpoint
/app/superset/
tekton/php



Apache Superset

- JWT с правами all_database_access
- SQL Injection для доступа к служебным БД



Access to Zabbix

- Нестандартный вход
- Получение логина и пароля Zabbix

Перемещение внутри периметра сети

Защита

- РТ EASM обнаруживает внешнюю уязвимость за 71 день до атаки (CWE-1220, CWE-89, CWE-266)

Кейс № 1.

Атака через мисконфигурации



Атака

Цепочка атаки через внешнюю уязвимость



SSO endpoint
/app/superset/
tekton/php



Apache Superset

- JWT с правами all_database_access
- SQL Injection для доступа к служебным БД

Перемещение внутри периметра сети



Access to Zabbix

- Нестандартный вход
- Получение логина и пароля Zabbix

Защита

- РТ EASM обнаруживает внешнюю уязвимость за 71 день до атаки (CWE-1220, CWE-89, CWE-266)
- За два дня до атаки РТ X выявил отсутствие агента EDR, даны рекомендации по его установке

Кейс № 1.

Атака через мисконфигурации



Атака

Цепочка атаки через внешнюю уязвимость



SSO endpoint
/app/superset/
tekon/php



Apache Superset

- JWT с правами all_database_access
- SQL Injection для доступа к служебным БД

Перемещение внутри периметра сети



Access to Zabbix

- Нестандартный вход
- Получение логина и пароля Zabbix



Access to Target server

- Доступ через Zabbix
- RCE и установка tools
- Exfiltration data



Password spraying to DC

- Подбор паролей в Active Directory

Защита

- РТ EASM обнаруживает внешнюю уязвимость за 71 день до атаки (CWE-1220, CWE-89, CWE-266)
- За два дня до атаки РТ X выявил отсутствие агента EDR, даны рекомендации по его установке

Кейс № 1.

Атака через мисконфигурации



Атака

Цепочка атаки через внешнюю уязвимость



SSO endpoint
/app/superset/
tekon/php



Apache Superset

- JWT с правами all_database_access
- SQL Injection для доступа к служебным БД

Перемещение внутри периметра сети



Access to Zabbix

- Нестандартный вход
- Получение логина и пароля Zabbix



Access to Target server

- Доступ через Zabbix
- RCE и установка tools
- Exfiltration data



Password spraying to DC

- Подбор паролей в Active Directory

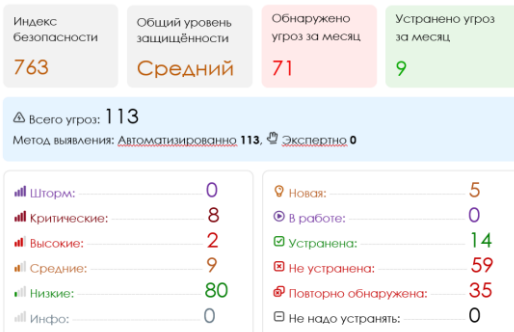
Защита

- PT EASM обнаруживает внешнюю уязвимость SSO endpoint с недостаточной фильтрацией пользовательского ввода за 71 день до атаки (CWE-1220, CWE-89, CWE-266)
- На сервере Zabbix, с которого развивается атака, не установлен агент MaxPatrol EDR
- PT NAD выявляет в сетевом трафике нестандартные SQL-запросы к целевому серверу. Формируется критический инцидент
- MaxPatrol EDR выявляет технику Password Spraying

PT EASM в PT X



Итоги анализа



NetSlicer

Интеллектуальный OSINT-агент для картографирования внешнего периметра: доменов, IP-адресов, сертификатов, связей



TuShcan (Cokmap)

Комплекс ускоренных ML-сканеров портов и приложений

97% точности при 1–2% трафика от брутфорса



OnoTolle AI

Автоматический триаж и группировка уязвимостей, снижение шума, генерация задач



Dirbruter, Authbruter, Domain Auditor

Модули перебора директорий, учетных данных и инструмент отслеживания сроков владения доменами



Offensive SOC

Непрерывный пентест с участием экспертов. Углубляемся в инфраструктуру и добираемся до сложных цепочек

Кейс № 2.

Детект атаки



Первоначальный
доступ

Закрепление

Разведка

Учетные данные

Компрометация
домена

Перемещение
внутри периметра

Закрепление

Кейс № 2.

Детект атаки



Первоначальный доступ	Закрепление	Разведка	Учетные данные	Компрометация домена	Перемещение внутри периметра	Закрепление
Start_Process_From_MOTW_Archive Запуск файла из ZIP-архива, полученного из внешнего источника	Cobalt_Strike_Powershell_Stager Загрузка и запуск полезной нагрузки Cobalt Strike через PowerShell	SharpHound_LDAP_Requests Массовые LDAP-запросы SharpHound для разведки объектов и связей Active Directory	Kerberoasting Запрос TGS-билетов для подбора пароля сервисной учетной записи	DCSync_Attack Имитация контроллера домена для получения учетных данных пользователей	Evil_WinRM_Activity Удаленное выполнение команд через Evil-WinRM	ShadowCred_Used Авторизация через shadow credentials без использования пароля

Кейс № 2.

Детект атаки



 MaxPatrol EDR  PT Sandbox	 MaxPatrol EDR	 MaxPatrol EDR  MaxPatrol SIEM  PT NAD	 MaxPatrol EDR  MaxPatrol SIEM  PT NAD	 MaxPatrol EDR  MaxPatrol SIEM  PT NAD	 MaxPatrol EDR  PT NAD	 MaxPatrol EDR
Первоначальный доступ	Закрепление	Разведка	Учетные данные	Компрометация домена	Перемещение внутри периметра	Закрепление
Start_Process_From_MOTW_Archive Запуск файла из ZIP-архива, полученного из внешнего источника	Cobalt_Strike_Powershell_Stager Загрузка и запуск полезной нагрузки Cobalt Strike через PowerShell	SharpHound_LDAP_Requests Массовые LDAP-запросы SharpHound для разведки объектов и связей Active Directory	Kerberoasting Запрос TGS-билетов для подбора пароля сервисной учетной записи	DCSync_Attack Имитация контроллера домена для получения учетных данных пользователей	Evil_WinRM_Activity Удаленное выполнение команд через Evil-WinRM	ShadowCred_Used Авторизация через shadow credentials без использования пароля

Кейс № 2.

Правила обнаружения



BASE

977

PT X



PRO

1721

Кейс № 3.

Скорость — ключевой фактор



07:55

Detect

CAP_DNS_Request_t
o_Suspicious_Domain

08:03

Analysis

Эскалирован
на 2-ю линию

08:19

Investigate

AI-расследование
и обогащение

08:40

Confirmed

Инцидент
подтвержден

08:52

Responded

Реагирование
на EDR-агенте

Кейс № 3.

Скорость — ключевой фактор



07:55

Detect

CAP_DNS_Request_to_Suspicious_Domain

- Выполнен DNS-запрос к подозрительному домену virtual****.ngrok.io
- Инцидент зарегистрирован в IRP
- Уровень опасности: **Medium**

08:03

Analysis

Эскалирован на 2-ю линию

- Проведен первичный AI-анализ, собраны и проанализированы похожие инциденты
- Инцидент агрегирован и эскалирован

08:19

Investigate

AI-расследование и обогащение

- Осуществлен сбор контента и его первичный анализ для аналитика. Подготовка вердиктов
- Инцидент проанализирован, подготовлены рекомендации

08:40

Confirmed

Инцидент подтвержден

- Инцидент подтвержден экспертом.
- План реагирования сформирован
- Уведомление направлено клиенту

08:52

Responded

Реагирование на EDR-агенте

- Зануление домена *.ngrok.io на конечном узле
- Инцидент закрыт

Кейс № 3.

AI-дежурные



Alerts Count (AC)

(поток инцидентов)

1431 → 3701

Queue Wait Time (QWT)

(медианное время нахождения в очереди)

11 → 1

Time To Investigate (TTI)

(медианное время до вынесения вердикта)

26 → 23

Alngela

- Первичная диагностика на легитимность
- Сбор похожих инцидентов
- Эскалация на человека

AI Colombo

- Анализ инцидента в режиме рассуждения
- Оценка риска
- Рекомендации по дальнейшим действиям

Технологии РТХ



Работа с уязвимостями до атаки

Перекрывающие контроли для
выявления угроз

Автоматизация анализа для повышения
скорости реакции



Спасибо!